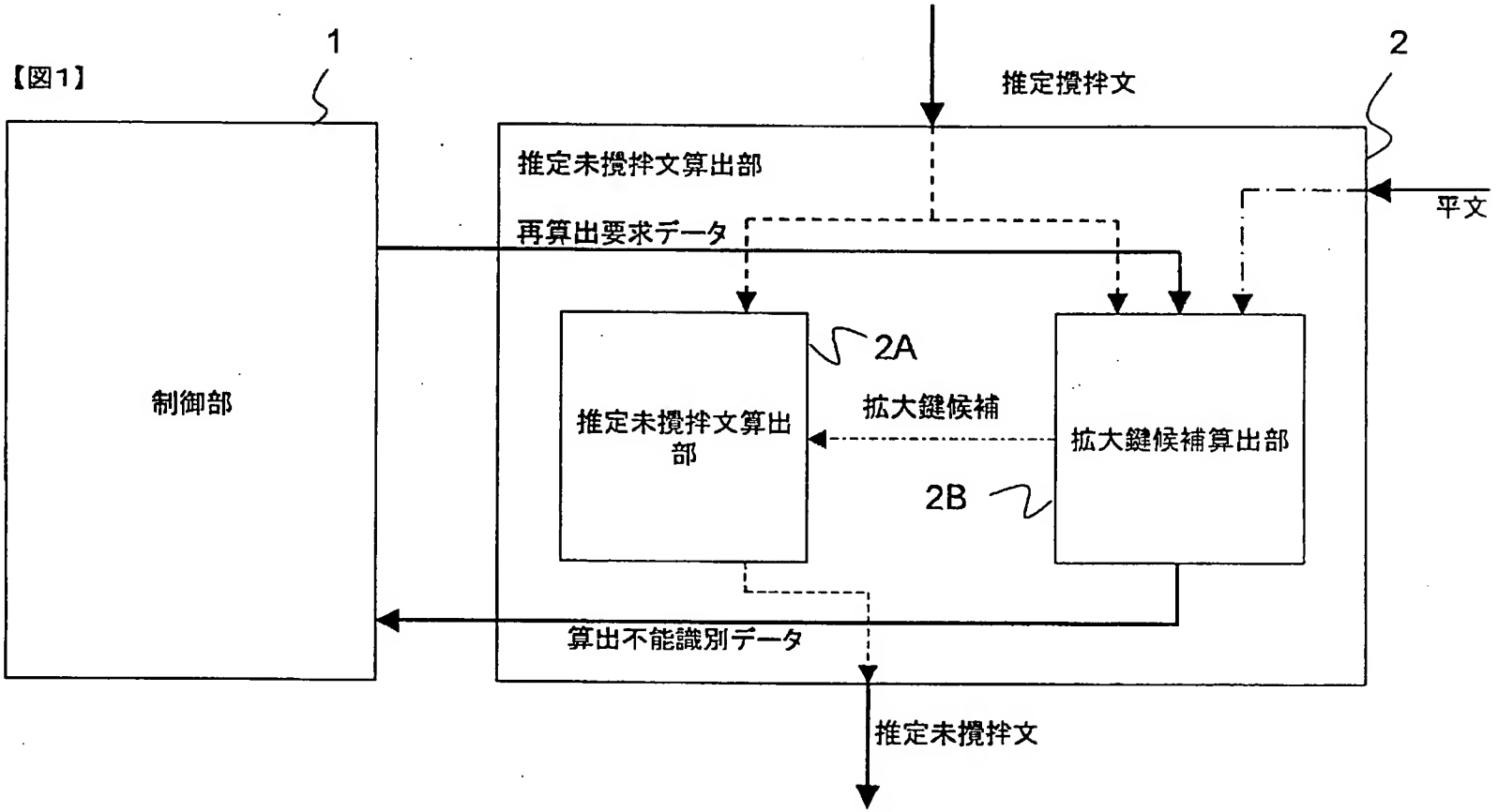
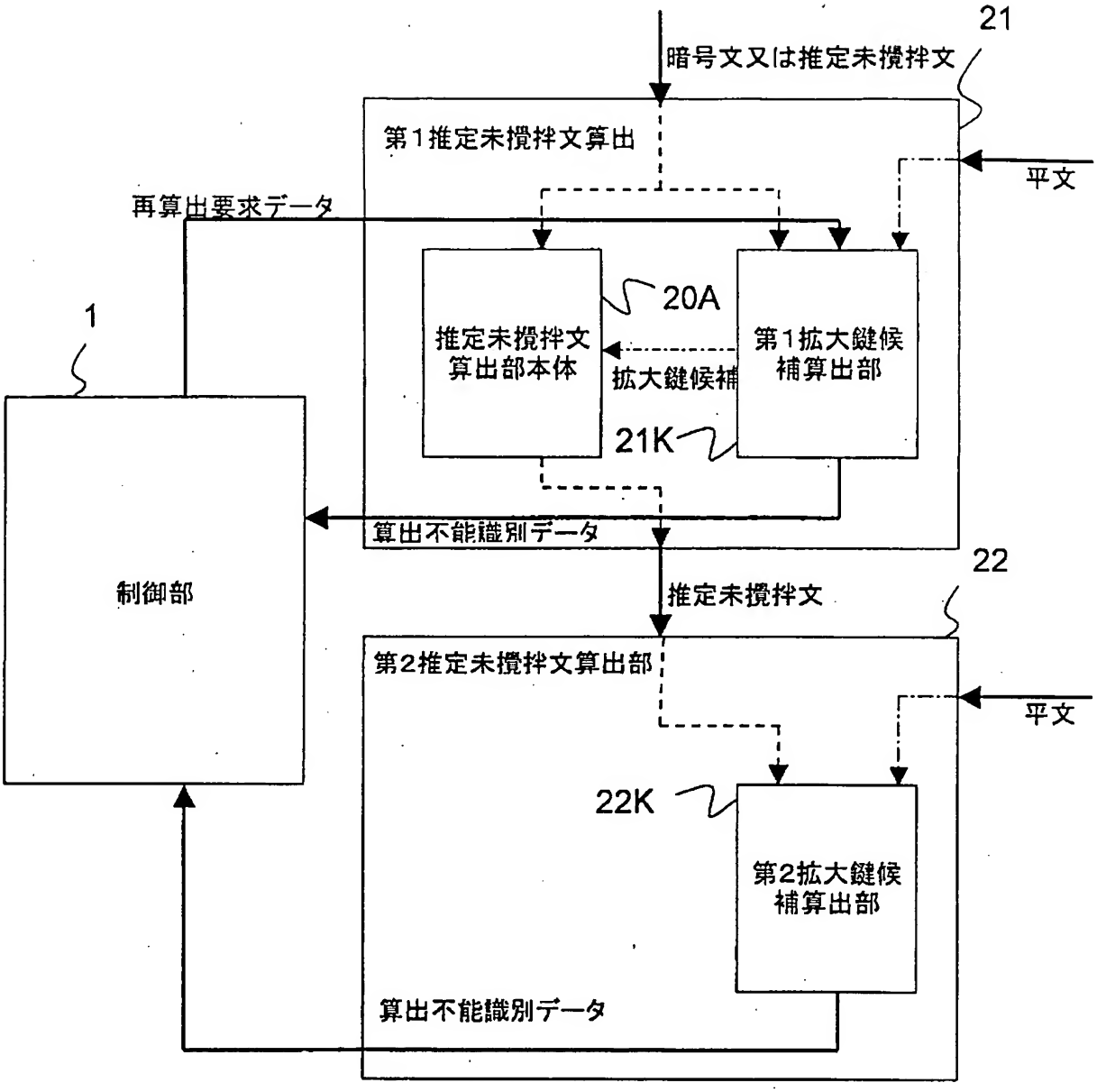
JC25 Rec'd PCT/PTO 29 JAN 2004

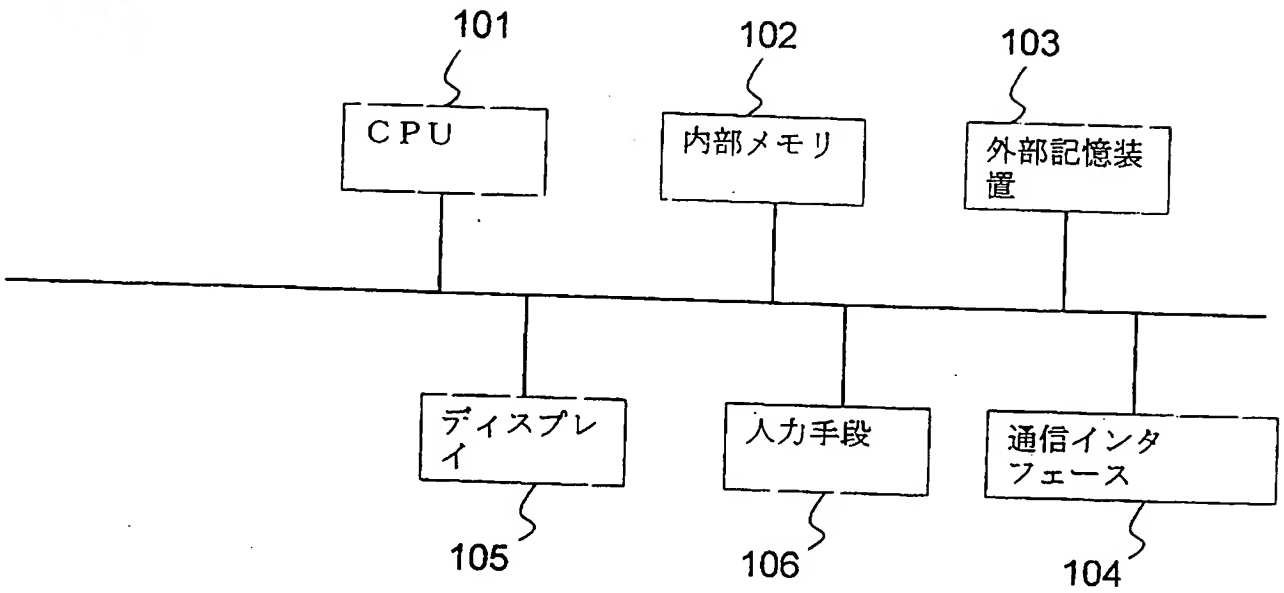
【図1】



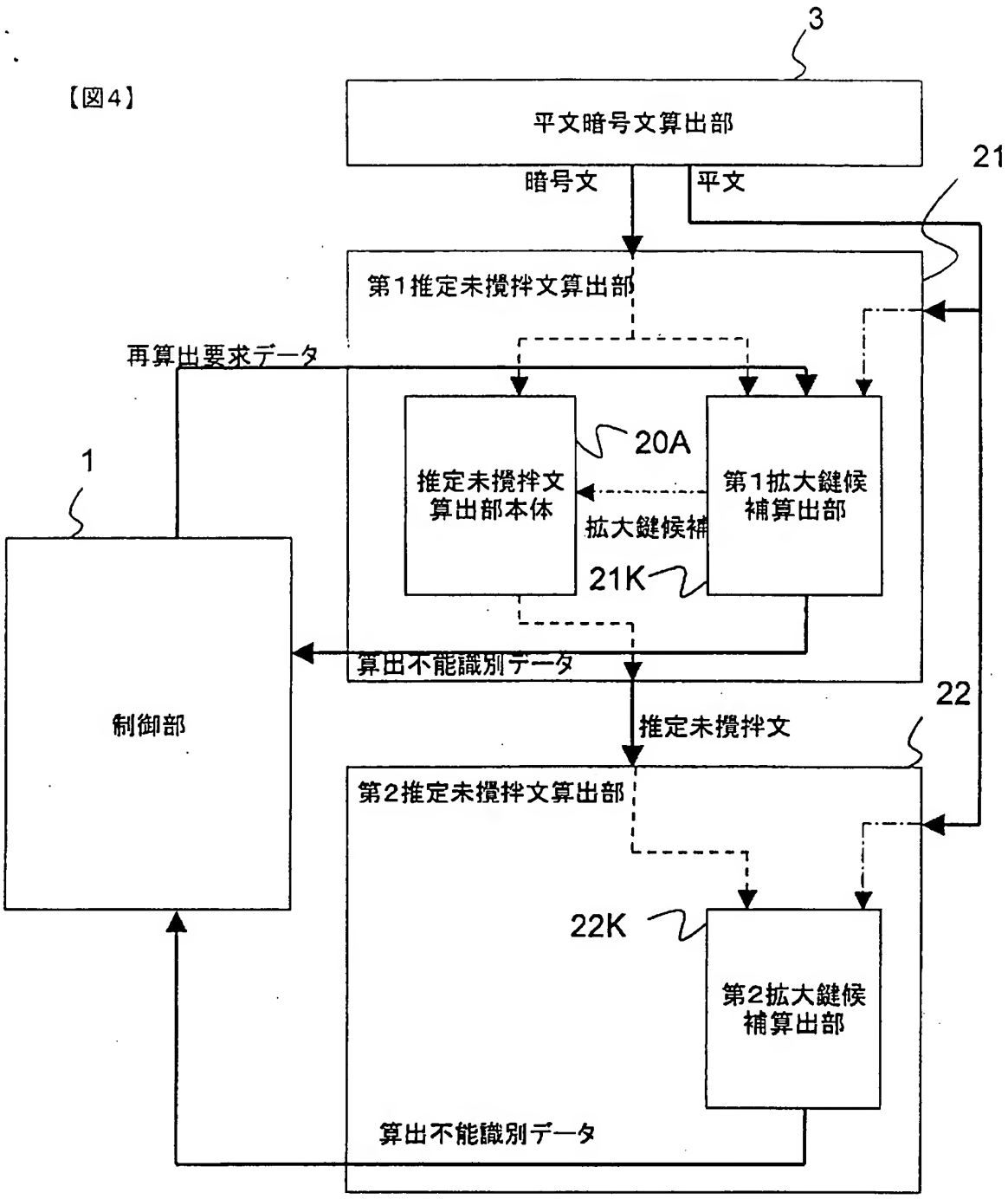
【図2】


21
暗号文又は推定未攪拌文
第1推定未攪拌文算出
平文
再算出要求データ
20A
推定未攪拌文
算出部本体
第1拡大鍵候
補算出部
1
拡大鍵候補
21K
算出不能識別データ
制御部
22
推定未攪拌文
第2推定未攪拌文算出部
平文
22K
第2拡大鍵候
補算出部
算出不能識別データ

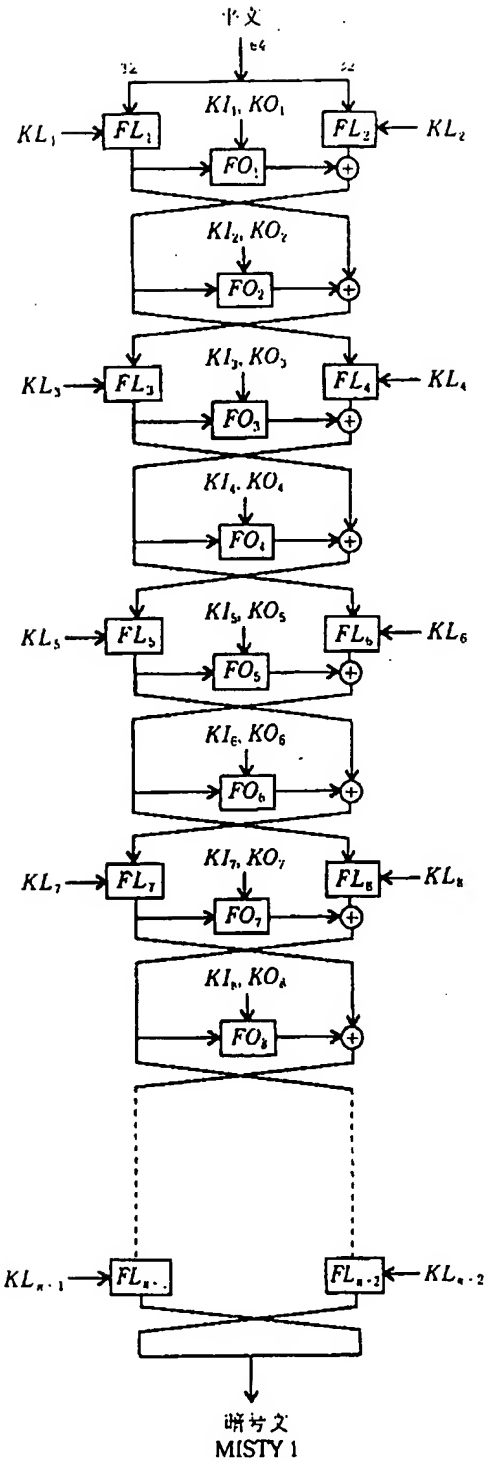
【図3】


101
CPU
102
内部メモリ
103
外部記憶装置
ディスプレイ
105
入力手段
106
通信インタフェース
104

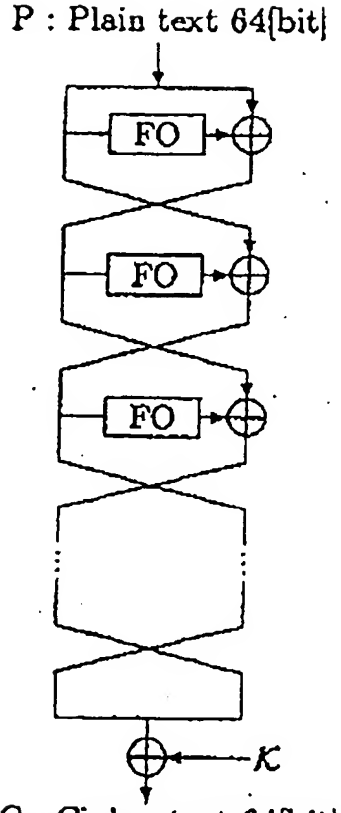
【図4】


3
平文暗号文算出部
暗号文
平文
21
第1推定未攪拌文算出部
再算出要求データ
20A
推定未攪拌文
算出部本体
第1拡大鍵候
補算出部
拡大鍵候補
21K
1
制御部
算出不能識別データ
22
推定未攪拌文
第2推定未攪拌文算出部
22K
第2拡大鍵候
補算出部
算出不能識別データ

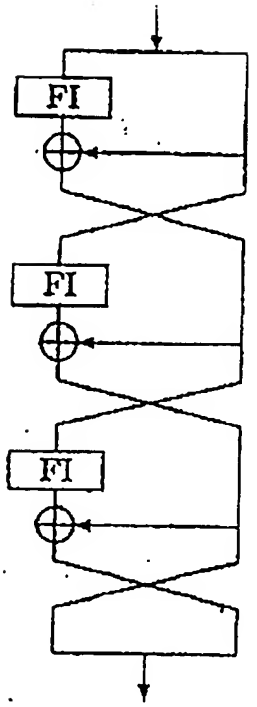
【図5】


平文
64
32
32
KI_1, KO_1
KL_1
FL_1
FL_2
KL_2
FO_1
KI_2, KO_2
FO_2
KI_3, KO_3
KL_3
FL_3
FL_4
KL_4
FO_3
KI_4, KO_4
FO_4
KI_5, KO_5
KL_5
FL_5
FL_6
KL_6
FO_5
KI_6, KO_6
FO_6
KI_7, KO_7
KL_7
FL_7
FL_8
KL_8
FO_7
KI_8, KO_8
FO_8
KL_{n-1}
FL_{n-1}
FL_{n-2}
KL_{n-2}
暗号文
MISTY 1

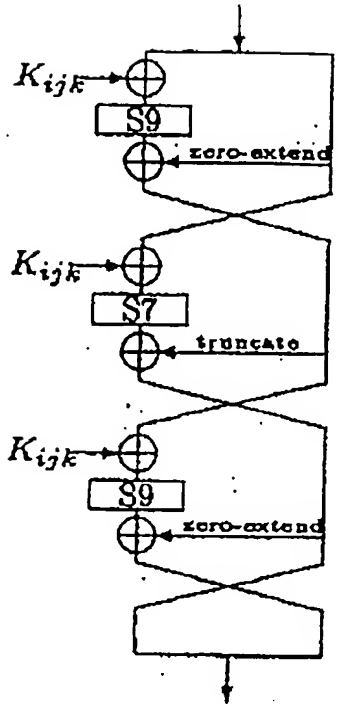
【図6】



(i) MISTY without FL

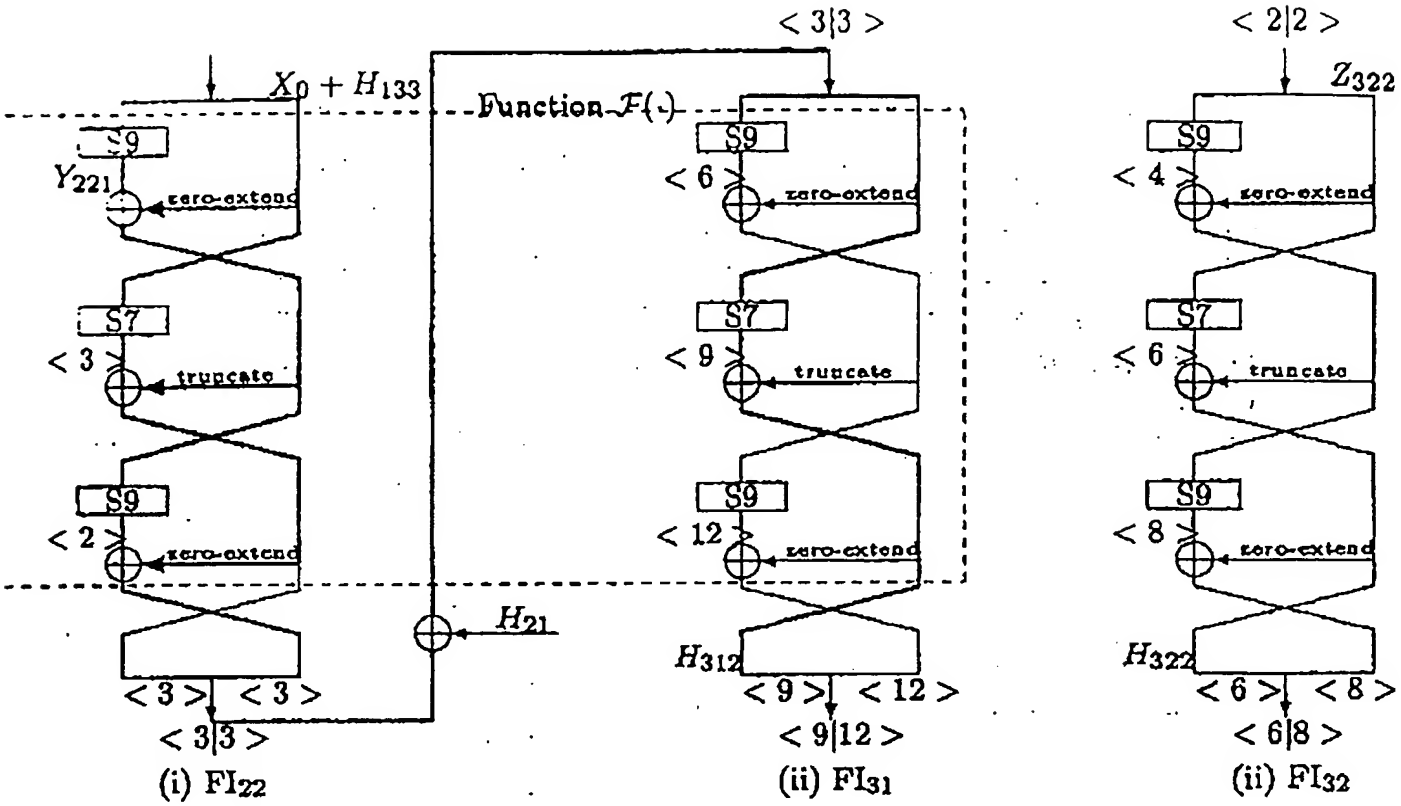


(ii) Equivalent FO



(iii) Equivalent FI

【図7】


$X_0 + H_{133}$
Function $\mathcal{F}(\cdot)$
< 3|3 >
Y_{221}
S9
zero-extend
S7
truncate
< 3 >
< 2 >
H_{21}
< 3 > < 3 >
< 3|3 >
(i) FI_{22}
< 6 >
< 9 >
< 12 >
H_{312}
< 9 > < 12 >
< 9|12 >
(ii) FI_{31}
< 2|2 >
Z_{322}
< 4 >
< 8 >
H_{322}
< 6 > < 8 >
< 6|8 >
(ii) FI_{32}